

DEMATERIALIZED MONIES – NEW MEANS OF PAYMENT

Alexandru Pîrjan and Dana - Mihaela Petroșanu *

Abstract

In this paper, we will outline the financial context in which the main means of payment dematerialization occurs. We will present the main characteristics of these new types of dematerialized monies: electronic money, virtual money, digital money, private money, purses and holders

Keywords:

Means of payment, dematerialized monies: electronic, virtual, digital, private, purses and holders.

Introduction

The first dematerialized currencies have appeared in the 1980s, due to an increased use of prepaid cards in telephony. We can perceive three types of dematerialized money: electronic money, virtual money and digital money.

The economic value of electronic money is measured in classical economic units (fiduciary) which must be stored in an electronic device accessible by the consumer. They represent actually scriptural money under binary form which is stored on a smartcard or on another portable device. The status of the issuer and the traceability of the transactions gives the scriptural character of the electronic monies. One can buy new units of payment either with classical money or through a bank account. The transactions are limited to the merchants who support them. Because electronic money does not represent legal tender or have discharging power, many experts consider that they do not have a straight existence.

Virtual money does not have tangible modes of payment, this being the main difference in respect to electronic money. Virtual monies are stored in software programs which allow transactions to be carried out on open network like the Internet. Virtual money can be regarded as a reference to a bank account. The status of the issuer and the traceability of the transactions give the scriptural character of the virtual money. In some cases virtual money can be also represented by virtual tokens or jetons, which are accepted only in a restricted commercial circuit. The jetons are issued only by trusted services providers and are tied with their banking accounts. A special case is when virtual money are

* Alexandru Pîrjan is at the Faculty of Computer Science for Business Management, Romanian American University in Bucharest.

Dana-Mihaela Petroșanu is at the Department of Mathematics I, University Politehnica of Bucharest in Bucharest.

issued by telephone companies under the form of prepaid cards whose value is meant for the payment of the company's services. In the future, telephone companies may have an intermediary role in e-commerce especially in the case of micropayments because they have developed to handle efficiently small payments and for settling accounts. In order for this to happen, a transition from 'virtual purse' to 'electronic purse' must take place so that the value stored in the prepaid card be recognized as a new universal type mean of payment. Another problem would be their regulation by the financial authorities.

In the case of digital money the value is stored under the form of algorithms on a hard disk, in a smartcard or in the memory of the user's computer and each piece is identified by an individual serial number. In order to achieve an efficient dematerialization of money, digital money must have a monetary sign, an authentic economic discharging power that will be accepted by most economic agents, the exchanging of values taking place over a network in real time by means of coded digital coins and their clearance and settlement may be achieved in real or non-real time. After having being verified their authentication, against a centralized or distributed authentication database, the digital money can be exchanged in physical money at different banks. Digital money allow a complete anonymous transaction by separating the payment from the user's identity, but it also has a major drawback, that of creating new universal monies, which are independent from current monetary system. For this reason, digital money has had a lot of technical and legal obstacles. An international digital currency would perturb existing economy and interfere with regional and local currencies. Delicate problems regarding national sovereignty could make their implementation almost impossible to achieve.

Electronic purses

An electronic purse consists of a rechargeable multipurpose prepaid card which can be used either for face-to-face payments or for retailing ones. Electronic purses are actually a substitute for other types of money. They represent portable electronic stores containing a precharged value, containing the funds owned by the cardholder. One of the most important security aspects of the electronic purses is that they are impossible to fake. Their use depends on legal regulations and on the identity of the issuer. In order for banking networks to be considered 'opened', the electronic money has to correspond to a legal currency. This is the reason why a purse which has been issued by a non-bank can only contain jetons and can only be used in restricted circles. Jeton holders are designed for use in certain closed situations just like private means of payments (prepaid telephone cards), which can be used to pay for telecommunication services. The banks find these electronic purses very appealing as they allow for a reduction of the transaction's cost and can even replace classical coins, notes and

cheques when small amounts are involved. Electronic purses have proved their usefulness in both face-to-face commerce and when making payments using automatic machines. Traditional payment cards are not suited to face-to-face commerce and micropayments because the cost of the transaction may exceed the actual amount.

Characteristic	Electronic Purse	Electronic Jeton Holder
Expression of purchasing power	Legal tender	Consumption unit
Unit of payment	Universal: can settle any payment in a defined territory	Specific to transactions involving the issuer
Guarantor of purchasing power	Bank	Service provider
Charging of value	By a bank or its agent	Unregulated
Circuit of financial services	Open	Closed

Figure 1. Comparison between electronic purses and electronic jeton holders.

An interesting approach would be the use of both electronic purses and jeton holders in a multipurpose card. In Figure 1 you can see the main financial and legal differences between electronic purses and electronic jeton holders.

Virtual purses

One can see a virtual purse as a precharged account with units of legal money and stored at a non-bank entity. The client can access online the virtual purse using special software installed on a personal computer. Services providers open more subaccounts in their banks and inside their own accounts. The clients or the merchants subscribe to one of these subaccounts. Because the stored value is physically intangible, the purse is “virtual”, but its payment units represent legal tender. The virtual purse is linked to the subaccount and it contains the purchasing power of the client. All clients have a copy of the balance on their personal computer and specific files that are used in cryptographic algorithms necessary for security reasons. Even in the case of a computer failure the assets of the clients are protected. The virtual purse of the client is debited while the merchant’s one is credited with the value of the transaction minus the commission which goes to the

operator. The transaction's cost in the case of micropayments is greatly diminished by the grouping of payments before the clearing.

The properties of transactions which use dematerialized currencies

All the transactions which use dematerialized currencies must respect several properties:

1. Atomicity: in order to have consequences a transaction has to complete all its states. If this doesn't happen, the previous transaction's state has to be restored.
2. Consistency: the critical aspect of the exchange must be accepted by all parties involved in the transaction.
3. Isolation: there mustn't be any interference among transactions.
4. Durability: if a breakdown do occurs, the system must return to its previous state.
5. Anonymity: revealing the buyer's identity is not mandatory when settling the obligations. On the other hand, personalization supposes that the identity of the buyer is known in order to be able to customize the offer.
6. Non-traceability: besides anonymity, this property means that one shouldn't be able to link two payments made by the same person.

Transactional properties of different means of payment is depicted in figure 2.

Property	Cash	Cheques	Credit transfer	Direct debit
Atomicity	Yes	Yes	Yes	Yes
Consistency	Yes	Yes	Yes	Yes
Isolation	Yes	No	Yes	Yes
Durability	Yes	Yes	Yes	Yes
Anonymity	Yes	No	No	No
Traceability	No	Yes	Yes	Yes
Property	Debit card	Credit card	Electronic purse	Virtual purse
Atomicity	Yes	No	Yes	Yes
Consistency	Yes	Yes	Yes	Yes
Isolation	Yes	Yes	Yes	Yes
Durability	Yes	Yes	Yes	Yes
Anonymity	No	No	Maybe	Maybe
Traceability	Yes	Yes	Maybe	Maybe

Figure 2. Transactional properties of different means of payment.

Because there are a lot of payment instruments, not all of them are suited to all the applications. This is an aspect which must be considered carefully when implementing new payment instruments in different societies. In order to obtain cash, cheques are used very often and in order to recharge a checking account cash is most often used. In contrast, besides cash, an electronic purse can be recharged from a checking account and even through a bank card, but the monies

can't be discharged in any of this forms. In figure 3 we present the money flow between an electronic purse and other means of payment.

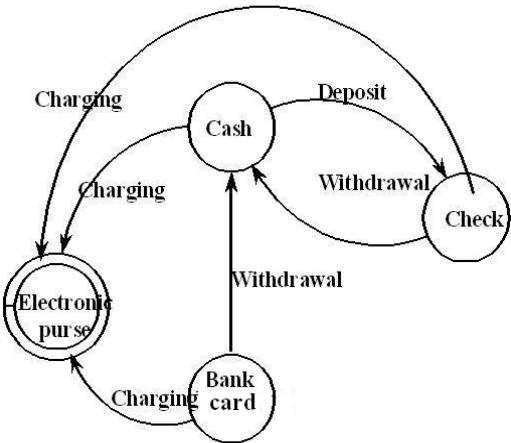


Figure 3. Monetary flow among payment instruments.

The various means of payments have different domains where they can be used. Cash is usually used in face-to-face payments, cheques are used in all cases of payments: face-to-face, remote and business-to-business, credit transfer is used in remote payment and business to business, while direct debit and interbank transfer are suited only in remote payments. Bank card can be used both in business to business and face-to-face payments but a card reader is required in this case.

Type of Money	Nature of Money	Support (the container)	Value Store
Fiduciary	Concrete, material	Paper, piece of metal	Safe, wallet, purse
Scriptural	Immaterial (maintained by a credit institution)	Magnetic, optical, electronic	Account maintained by a credit institution
		Integrated circuit card	Electronic purse
		Computer	Virtual purse (memory allocated by an intermediary)
Type of Money	Value Representation	Mode of Payment	Means of Payments (Instrument)
Fiduciary	Bank notes, coins	Face-to-face transaction	Bank notes, coins
Scriptural	Numerical value	Remote, face-to-face (retail automatic machines)	Check, debit card, credit card, credit transfer
			Electronic fund transfer

Figure 4. Comparison of monies.

Electronic or virtual purse is used with a card reader in face-to-face payments and it might also be used in remote and business to business payments.

Various properties of money and a comparison between them is depicted in figure 4. This evaluation is made by taking into account several criteria : the nature of money, their support, the way how the value is stored and represented, the mode and the means of payment.

The financial and control flow between participants in a system of dematerialized money is presented in figure 5.

The operator is responsible for charging the purse with electronic monetary units and he has an interface with the client presented in relation 1. The operator must verify the financial status of the holder or the validity of payments made by using classical means of payment. After having verified the electronic or virtual purse, the operator puts up-to-date their stored value.

If the charging operator is not a bank, there must be a connection between him and the issuing bank, as presented in figure 5 as relation 2.

The issuing bank must also communicate to the acquiring bank (the merchant's bank), respecting the necessary regulations. This is marked as relation 3.

Relation 4 shows that in order to acquire the merchant's credit, the acquiring operator exchanges information with the acquiring bank.

The corresponding values of the electronic transactions are collected and compensated for crediting the merchant's account, just like it is presented in relation 5.

Relation 6 shows that the transfer of electronic value from the client to the merchant's account is done simultaneously during a purchase.

The charging protocol represents a set of procedures for processes regarding authorization and transfer of electronic value to the owner's purse corresponding to a payment accepted by the charging operator. Protocols must assure a reliable security so that they will resist to outside attacks. The messages should be available only to the participants, a third party which is not a participant should not be able to access, manipulate or to modify these messages.

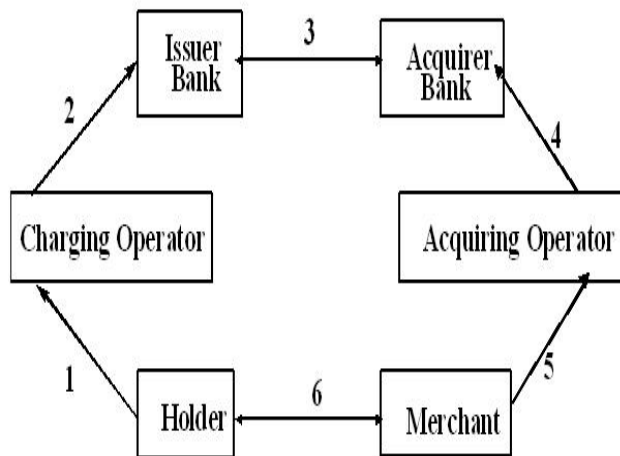


Figure 5. Flows in a transaction by dematerialized money.

The protocols must assure that the charges are authentic and they should prevent a false server from debiting a purse, the recharge of an unidentified purse, recharging with a different amount, other than the one requested, should prevent replay a tax (such as a previous authenticated value be recharged more times) and it should also be able to prevent the repudiation of a charge which has been correctly executed or a payment which has been made. The protocols should offer the possibility to return to the previous state in case a transmission error occurs.

The case of direct payments made to the merchant

If the payment is directly made to the merchant, the clients have to send the details of their accounts. In order to assure the security of the banking network from the Internet traffic, a payment gateway must be used when making payments from the client's computers by means of a purse or a bank card.

The gateway will get and handle the client's request, and so the gateway operator can be seen as a trusted third party. In order for the gateway operator to be a charging operator, it must be certified by a credit institution. In figure 6 one can observe a location of the payment gateway in electronic commerce.

Due to the large number of projects for electronic purses implemented around the world, a lot of incompatibility problems have emerged.

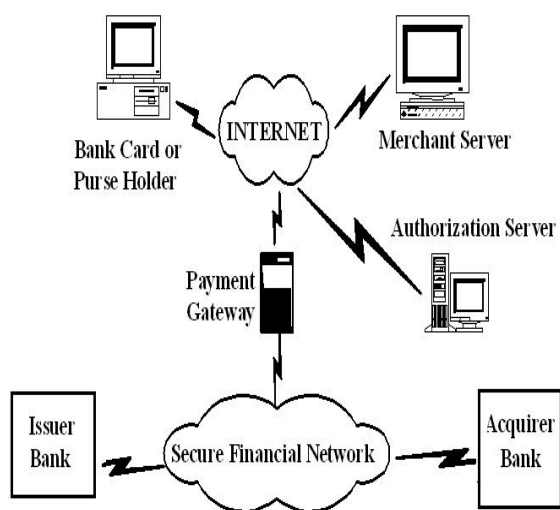


Figure 6. Payment gateways in electronic commerce

An important step in consolidating an unique payment interface is the Electronic Commerce Modeling Language (ECML), described in IETF RFC 3106, which defines how the exchanges between applications and the merchant's site should take place. A digital wallet is a software that manages the details of an online order.

A major disadvantage of the direct payments is that the merchant and the cardholder have to come upon all the details of the protocol which they use, and this represents an impediment for open exchanges. Most of the payment schemes that could be used must be supported by the merchant's site. For each currency the customer would have to own a purse and due to its cost these could be a serious inconvenience. One solution for overcoming some of these drawbacks is the payment be mediated by intermediaries.

Payments through an intermediary

In figure 7 we present the position of the payment intermediary in the e-commerce circuit.

The intermediary levels the differences among the various purse schemes in regard with the participants, allowing them to overcome the burden of having specific software for different systems of payment. In order to access the intermediary's gateway, the client must subscribe to this service.

There are two cases: one when the payment will be done by bank card or electronic purse and another when the payment is done through a virtual purse.

In the first case the intermediary usually knows the client's details as they have been previously send through a secure channel. Using this information, the intermediary instructs the banking authorities to debit the buyer's account for the purchases he has made and to credit the supplier with the respective amounts. The holder uses an identifier (that could be encrypted with a secret key) in order to establish a connection.

In the second case the intermediary opens more subaccounts in it's own bank for the users and merchants which subscribe to its services. By means of direct credit or by a bank card the users prepaid their subaccounts. The transactions are grouped and are settled periodically with the banking network after having withdrawn their commission.

The are many services which an intermediary can offer such as: the management of a virtual mall and the payment instrument for the merchant, can take care of exchange rates, import and export taxes, shipping of physical goods, etc. The intermediary has to manage the generation, distribution, archiving and revocation of the encryption keys, the subscriptions of merchants and clients, and must also updates the directories and the black list or revocation list. A nonrepudiation service which timestamps the exchanges can also be implemented.

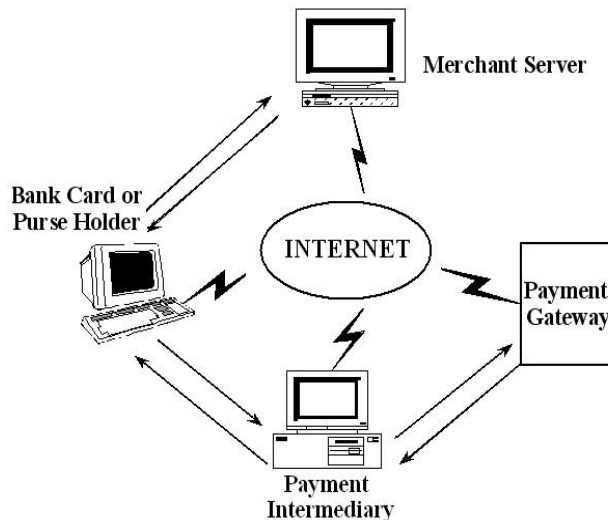


Figure 7. Payment intermediaries in electronic commerce

If the intermediary is a telephone company, we can see the telephone unit as a virtual money unit, which is used between the supplier and the client in micropayments. This can be very useful if the two parties involved are not from the same country.

Important administrative functions could be also fulfilled by intermediary for example the paying of taxes in France, where the DGI (Direction Générale des

Impôts – General Taxation Directorate) certifies certain service providers to act as a relaying organization that can send fiscal data according to the law. The intermediary gives its clients the possibility of signing electronic documents. Using the RSA algorithm the public DGI's key is used to encrypt the digest of the document and the symmetric key. Starting from 2000 a fiscal declaration can be sent to the fiscal institutions only by EDI partners, according to EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) .

Clearing and settlement

The process in which banks are settling the accounts by exchanging money is referred as “clearing and settlement”. The respective values are analyzed, compared and the accounts are settled in a special clearing house every working day. When talking about electronic and clearing settlement the process is done over computer network.

Several different models for clearance and settlement systems exist in Europe, but differ from country to country in respect with the unique evolution of the financial circuits, different views over security issues, and the diversity of standards from each of these countries.

We can make a classification of the settlement networks taking into account several criteria like:

1. The dimension of the processing: there can be large value systems and mass systems that process many transaction of relatively small values on a daily bases.
2. The ownership of the managed network: the owner of the network can be the central bank in the case of a public network or more members of a group of banks in the case of a private network.
3. How the settlement is done: the settlement can take place in real time in the same day. In order to avoid the charges for settling the payment, grouping is used whenever the parties involved are from the same group of companies.

Conclusions

Many technical, political and social factors are involved in acceptance of a payment system. The existing architecture of the payment systems must be taken into account when a worldwide e-commerce solution has to be implemented.

Especially in the case of micropayments, intermediaries should be used for assuring a cost effective transaction's billing and collection of monies. These intermediaries should be able to act as a single proxy interface independent of the underlying scheme of the system's payment. The differences in currencies and the fluctuations of the exchange rates are important issues which must be dealt with in

the case of micropayments as they pose additional financial risk to all the participants.

References

Alexandru Pirjan 2005. “Electronic Mobile Commerce”, Information Systems & Operations

Management (Isom) Workshop No. 3, April 20 - 21, pp.171 - 178, ISBN – 973-87166-8-3.

Alexandru Pirjan. 2006. “Quality Evaluation of Electronic Commerce Web Sites Using The EWAM method”, *Information Systems & Operations Management (Isom) Workshop* No. 4, March 1-2, pp.218-227, ISBN – 973-7643-75-5.

Mostafa Hashem Sherif. 2004. *Protocols for Secure Electronic Commerce*, CRC Press, US.

Susan Hohenberger. 2006. *Phd Thesis*, Advances in Signatures, Encryption, and E-Cash from Bilinear Groups, *Massachusetts Institute of Tehnology*.

Victor Valeriu Patriciu. 2001. Monica Ene-Pietrosanu, Ion Bica, Calin Vaduva, Nicolae Voicu - Securitatea comertului electronic, *Editura BIC ALL, Bucuresti*.

Victor Valeriu Patriciu, Monica Ene-Pietrosanu, Ion Bica, Justin Priescu. 2006. Semnaturi electronice si securitate informatica, *Editura BIC ALL, Bucuresti*.